Cybersecurity and the Media: Misinformation and Public Perception

Topic 8

Alex Bretana, Brandon Rollinson, Caden West, John Monrouzeau, Jayden Egan

How Media can Harm Public Perception of Cybersecurity and Hacking

Media can significantly change the public's way of viewing cybersecurity and hacking. Some of the main ways it can cause harm are:

- Oversimplifying Hacking – Movies and TV shows make hacking seem like something done in seconds, with green letters flying all over the screen and overexaggerated fast typing.
- Sensationalizing Cyber Threats - Media outlets have a tendency of exaggerating the scale of cyberattacks to gain attention, which can lead to unneeded fear or the belief that ALL cyber threats are big threats, when they could actually be easily prevented.
- Encouraging false expectations of Cybersecurity - Medias make it look like cybersecurity experts are miracle workers, like being able to pinpoint a hacker on the other side of the world in seconds or make a system impenetrable. But the truth is, Cybersecurity can be a long and tedious process, involving long-term planning, constant monitoring of systems, and even investigations taking weeks or months.
- Accurate representations of Cybersecurity are important, because the public perception of it has already been harmed enough. A more accurate depiction could entice an uninterested person into pursuing a career in cybersecurity and boost the industry.

Swordfish (2001)

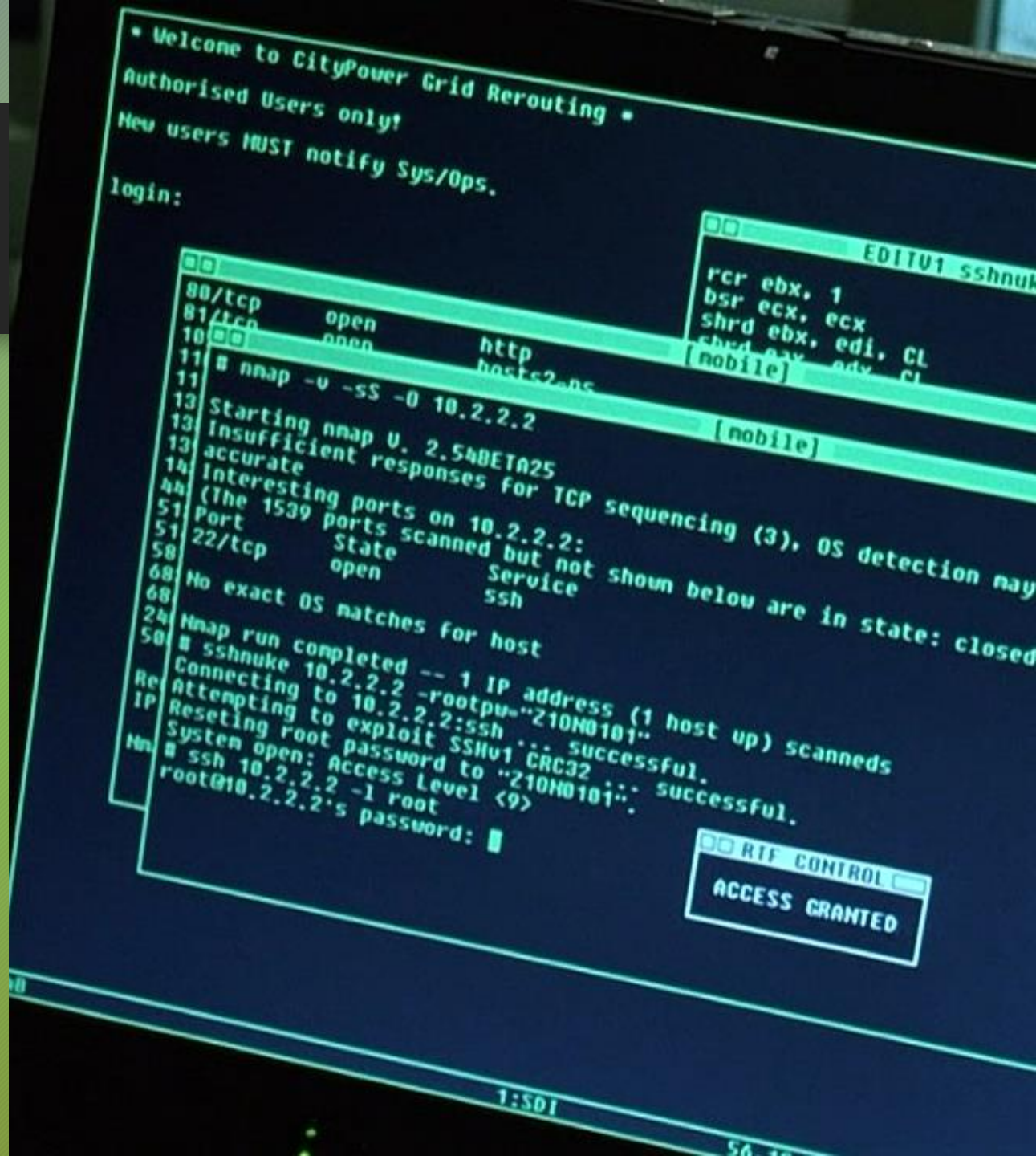
- https://youtu.be/u1Ds9CeG-VY?si=b9HwFcJ7pf1TiQRp
- The movie *Swordfish* turns hacking into a fake thriller trope. Hugh Jackman types near-gibberish into multiple CGI screens, including a 3D geometric object at the end showing the hack completing – something more fit for a futuristic sci-fi anime than a "realistic" movie.
- Throughout the movie, random corny cyber-jargon is used to make it seem more legitimate. Some examples are "slide in a trojan horse hiding a worm," and "DoD DES dBase, 128-bit encryption."
- What is DES 128-bit, you might ask? Well, it doesn't exist. DES was superseded by a new algorithm called Advanced Encryption Standard (AES) in 2001. AES does come in a 128-bit variety, but DES never has and never will - so, "this entire scene is 128 bits of B.S." (Cool, 2022)
- This over-the-top hacking was a common trope in the 90s and early 2000s that turned the common perception of hacking and cybersecurity into one of fast typing and crazy supercomputers with walls of green text.

Watch Dogs (2014)

- In the Ubisoft game series *Watch Dogs*, hacking is a main mechanic. It is portrayed as a simple smartphone app, that the main character uses to hack anything around them.
- With a press of a button, security cameras, traffic lights and bollards, and even vehicles themselves can be hacked. Any person walking by is scanned through their cell phone, and their name, age, occupation, etc, are scanned and shown. The entire city power grid can even be shut down with a single button press.
- This is a hyperbole of modern-day hacking, fantastically exaggerating it into this dystopian-style method – since the imaginary cities use mostly tech from a single company, it is easy to hack the whole network.
- This can be taken as a cautionary tale for our future and even current day lifestyles, filled with IoT devices, including Amazon Alexa, Ring doorbell cameras, etc. We fill our lives with poorly-secured devices that can act as vulnerabilities into our private lives.

A more Accurate Depiction- nmap used in *The Matrix (1999)*

- https://www.youtube.com/watch?v=0PxTAn4g20U
- In *The Matrix*, the character Trinity correctly uses the nmap function in a linux terminal to access the network of a power grid, also exploiting the "sshnuke" vulnerability of early OpenSSH version from the 90's. (Fyodor, 2020)
- Of course, after the few seconds of accuracy, it quickly devolves into sci-fi nonsense. Being one of the biggest blockbusters of the 90's and early 2000s, it heavily impacted the public's perception of deep computer usage and cyber-infiltration.
- The falling text graphics used in the credits from *The Matrix* became a staple image used in mentions of hacking, with a linux program even created to simulate it, called Cmatrix. Cmatrix has even been used in television news broadcasts as stock footage during coverage of hacking and ransomware attacks!

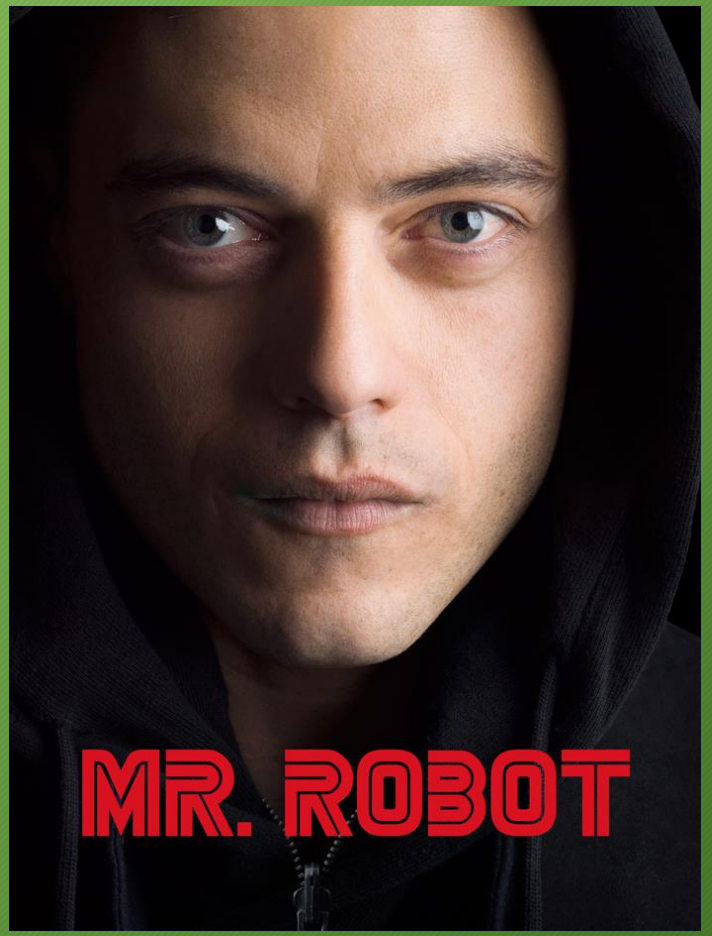


Person of Interest (2011)

- Person of Interest deals with hacking, surveillance, AI, data mining, and cyber operations. It has some dramatic elements, and it's known for being realistic in explaining the digital tracking and intelligence systems.
- This show highlights real-world cyber threats such as insider attacks, data breaches, and corporate spying, showing how easily trusted users or compromised systems can be exploited to harm people and corporations. The show also explains data exfiltration and system intrusions where infiltrated networks overlooked vulnerabilities.
- It shows AI realistically by showing how algorithms analyze massive amounts of data like in surveillance footage, metadata, and communication patterns to predict potential threats. Person of Interest also shows the ethical issue of advanced AI. Like giving a machine too much control over public surveillance.

Mr. Robot

- Mr. Robot is a show that is praised for its realistic depictions of topics like cybersecurity, hacking, digital privacy, and cyber operations. The show highlights how cyber threats, such as phishing and ransomware are easily able to compromise an entire network.
- Some prevent topics this show goes into includes ethical issues surrounding digital power, and the consequences that stem from mass surveillance and corporate control over data.
- Mr. Robot portrays different cyber operations tactics, such as password cracking and physical access attacks. It also explores how hackers use psychological manipulation techniques and misinformation to skew the public view and control an agenda.



Works Cited

- BBC. (2003, May 19). Matrix mixes life and hacking. *News.bbc.co.uk*. http://news.bbc.co.uk/2/hi/technology/3039329.stm
- CertLibrary. (2025, May 19). *An In-Depth Analysis of Hacking Realism in Mr. Robot - CertLibrary Blog*. CertLibrary Blog. https://www.certlibrary.com/blog/an-in-depth-analysis-of-hacking-realism-in-mr-robot/
- Cool, Z. (2022, April 27). *Swordfish*. Medium; h0llyw00d h4x0rs. https://medium.com/h0llyw00d-h4x0rs/swordfish-77a83716baa9
- Fyodor. (2020, April 21). *Movies Featuring the Nmap Security Scanner*. Nmap.org; nmap. https://nmap.org/movies/
- K, M. (2012). Person Of Interest - Pilot - The Beginning Part 2 [Mp4]. In *YouTube*. https://www.youtube.com/watch?v=iFp-L2sE-Io
- Runger-Field, L. (2024, September 24). *How Cybersecurity in Pop Culture Shapes Our Understanding of Digital Threats*. PIA VPN Blog. https://www.privateinternetaccess.com/blog/cybersecurity-pop-culture/
- Wikimedia Foundation. (2022, March 25). *Person of Interest (TV series)*. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/Person_of_Interest_(TV_series)